AMENDMENTS TO THE CLAIMS

Claims 1-34 are pending in the instant application. Claims 1, 2, 11, 12, 21 and 22 have been amended.

Listing of claims:

1. (Currently amended) A method for producing a secure key, the method comprising:

receiving at least a first input key, a second input key and a third input key; and

generating a first output key based on said at least said first input key, said second input key and said third input key, wherein said first output key is unique and differs from said at least said first input key, and said third input key is a key variation comprising a device identity.

2. (Currently amended) The method according to claim 1, wherein said first input key is a customer key, and said second input key is a customer key selection ~~and said third input key is a key variation~~.

3. (Previously presented) The method according to claim 1, comprising:

determining whether said first output key is at least one of a unique key and differs from said at least said first input key; and

if said first output key is at least one of a non-unique key and is equivalent to said at least said first input key, generating a second output key based on a modified one of at least one of said first input key, said second input key and said third input key.

4. (Previously presented) The method according to claim 3, comprising determining whether said second output key is at least one of a unique key and differs from said at least said modified one of at least one of said first input key, said second input key and said third input key.

5. (Original) The method according to claim 4, wherein said first output key and said second output key are not weak or semi-weak keys.

6. (Previously presented) The method according to claim 1, comprising mapping said at least said first input key, said second input key and said third input key to generate mapped output key data.

7. (Previously presented) The method according to claim 6, comprising generating an intermediate key based on said first input key.

8. (Previously presented) The method according to claim 7, comprising scrambling said generated intermediate key and said generated mapped output key data to create a scrambled output.

9. (Previously presented) The method according to claim 8, comprising:

masking at least a portion of said generated mapped output key data; and

exclusive ORing said masked at least said portion of said generated mapped output key data and said scrambled output to generate said first output key.

10. (Previously presented) The method according to claim 1, comprising transferring said generated first output key to an encryption engine that utilizes said generated first output key to encrypt information.

11. (Currently amended) A machine-readable storage having stored thereon, a computer program having at least one code section for producing a secure key, the at least one code section being executable by a machine for causing the machine to perform steps comprising:

receiving at least a first input key, a second input key and a third input key; and

generating a first output key based on said at least said first input key, said second input key and said third input key, wherein said first output key is unique and differs from said at least said first input key, and said third input key is a key variation comprising a device identity.

12. (Currently amended) The machine-readable storage according to claim 11, wherein said first input key is a customer key, and said second input key is a customer key selection ~~and said third input key is a key variation~~.

13. (Previously presented) The machine-readable storage according to claim 11, comprising:

code for determining whether said first output key is at least one of a unique key and differs from said at least said first input key; and

code for generating a second output key based on a modified one of at least one of said first input key, said second input key and said third input key if said first output key is at least one of a non-unique key and is equivalent to said at least said first input key.

14. (Previously presented) The machine-readable storage according to claim 13, comprising code for determining whether said second output key is at

least one of a unique key and differs from said at least said modified one of at least one of said first input key, said second input key and said third input key.

15. (Original) The machine-readable storage according to claim 14, wherein said first output key and said second output key are not weak or semi-weak keys.

16. (Previously presented) The machine-readable storage according to claim 11, comprising code for mapping said at least said first input key, said second input key and said third input key to generate mapped output key data.

17. (Previously presented) The machine-readable storage according to claim 16, comprising code for generating an intermediate key based on said first input key.

18. (Previously presented) The machine-readable storage according to claim 17, comprising code for scrambling said generated intermediate key and said generated mapped output key data to create a scrambled output.

19. (Previously presented) The machine-readable storage according to claim 18, comprising:

code for masking at least a portion of said generated mapped output key data; and

code for exclusive ORing said masked at least said portion of said generated mapped output key data and said scrambled output to generate said first output key.

20. (Previously presented) The machine-readable storage according to claim 11, comprising code for transferring said generated first output key to an encryption engine that utilizes said generated first output key to encrypt information.

21. (Currently amended) A system for producing a secure key, the system comprising:

a secure key generator that receives at least a first input key, a second input key and a third input key; and

said secure key generator generates a first output key based on said at least said first input key, said second input key and said third input key, wherein said first output key is unique and differs from said at least said first input key, and said third input key is a key variation comprising a device identity.

22. (Currently amended) The system according to claim 21, wherein said first input key is a customer key, and said second input key is a customer key selection ~~and said third input key is a key variation~~.

23. (Previously presented) The system according to claim 21, wherein said secure key generator:

determines whether said first output key is at least one of a unique key and differs from said at least said first input key; and

generates a second output key based on a modified one of at least one of said first input key, said second input key and said third input key, if said first output key is at least one of a non-unique key and is equivalent to said at least said first input key.

24. (Previously presented) The system according to claim 23, wherein said secure key generator determines whether said second output key is at least one of a unique key and differs from said at least said modified one of at least one of said first input key, said second input key and said third input key.

25. (Original) The system according to claim 24, wherein said first output key and said second output key are not weak or semi-weak keys.

26. (Previously presented) The system according to claim 21, comprising a mapper that maps said at least said first input key, said second input key and said third input key to generate mapped output key data.

27. (Previously presented) The system according to claim 26, comprising a key generator that generates an intermediate key based on said first input key.

28. (Previously presented) The system according to claim 27, comprising a scrambler that scrambles said generated intermediate key and said generated mapped output key data to create a scrambled output.

29. (Previously presented) The system according to claim 28, comprising:

a masker that masks at least a portion of said generated mapped output key data; and

an exclusive OR operator that exclusive ORs said masked at least said portion of said generated mapped output key data and said scrambled output to generate said first output key.

30. (Original) The system according to claim 21, wherein said secure key generator transfers said generated first output key to an encryption engine that utilizes said generated first output key to encrypt information.

31. (Original) A system for producing a secure key, the system comprising:

a mapper;

a scrambler coupled to said mapper;

a masker coupled to said mapper;

a key generator coupled to said scrambler; and

an XOR operator coupled to said masker and said scrambler.

32. (Previously presented) The system according to claim 31, comprising at least one processor coupled to an output of said XOR operator.

33. (Previously presented) The system according to claim 32, comprising an encryption engine that is coupled to an output of said XOR operator.

34. (Previously presented) The system according to claim 33, comprising a memory coupled to at least one of said encryption engine and said at least one processor.